CYBERSEC 2019

Programa preliminar (sujeto a modificaciones)

DIA 1
24 OCTUBRE

SALON PLENARIO LAS AMERICAS JUEVES 24 de Octubre	
08:00 - 09:00	Acreditación
09:00-09:15	Bienvenida. Fernando Rannou
09:15-09:45	ECOSISTEMAS DE CIBERSEGURIDAD DEL PACÍFICO SUR Senador Kenneth Pugh
09:45 – 10:30	GDPR GAME CHANGERS AND SOLUTION FOR COMPLIANCE. Keynote Speaker Danielle Catteddu. CSA. (Ponencia en Inglés)
10:30—11:00	CONVERGING IT-OT NETWORKS- THE POWER OF 100%VISIBILITY…. Alejandro Dutto- Forescout Technologies
11:00-11:45	Coffee Break- NETWORKING
11:45 – 13:00	MESA REDONDA: INFRAESTRUCTURA CRITICA. Modera: **Soledad Bastías** Integrantes de la mesa: **Katherina Canales**- Asesor legal en Ciberseguridad CSIRT de Gobierno **Helvecia Castro-** Directora de Seguridad de la Información ENAP **Jorge Baeza**- Gerente de Seguridad de la Información- Metro **Daniel Soto**- Responsable de Ciberseguridad- Naturgy
13:00 – 14:00	Almuerzo- Visita Exhibición
14:00 – 14:30	PROTECCIÓN Y ANONIMIZACIÓN DE DATOS EN ECOSISTEMAS HÍBRIDOS Sergio Muniz. Thales
14:30-15:00	BENEFICIOS DE UNA GESTIÓN INTEGRADA DE RIESGOS Miguel Aranguren- Assertiva
15:00 -15:30	MODELO DE CONFIANZA CERO, LA NUEVA FORMA DE COMBATIR LAS AMENAZAS AVANZADAS Ximena Tapia- Microsoft
15:30 – 16:00	CIBERSEGURIDAD: LA PIEDRA ANGULAR DE LA TRANSFORMACIÓN DIGITAL Orador por definir- Cisco
16:00-16:45	Coffee Break- NETWORKING
16:45-17:15	EL AWARENESS Y LA CULTURA ORGANIZACIONAL 3.0 Felipe Molina- 3IT
17:15 -17:45	ESTABLECIENDO PROGRAMAS DevSecOps QUE GENERAN RETORNOS TANGIBLES PARA EL NEGOCIO Edward Cook- Business Continuity
17:45 -18:15	LA IMPORTANCIA DE LA VISIBILIDAD EN LAS ESTRATEGIAS DE CIBERSEGURIDAD Juan Vergara- Gigamon
18:15 – 18: 45	APLICACIÓN DE TEORÍA DE CONTROL E INTRODUCCIÓN DEL CONCEPTO DE RETROALIMENTACIÓN PARA UN NUEVO PARADIGMA EN CIBERSEGURIDAD Ricardo Villadiego- Lumu Technologies

DIA 2
25 OCTUBRE

VIERNES 25 de Octubre	
08:00 – 09:00	Acreditación
09:00- 09:10	Bienvenida
09:10 – 09:55	INSIDE ATTACKS AND ZERO KNOWLEDGE NETWORKS Jochen Kressin- Search Guard (Ponencia en Inglés)
09:55 – 10:25	PONENCIA POR CONFIRMAR IBM
10:25 -10:55	LA PERSONA COMO EL ESLABÓN MÁS FUERTE DE LA CIBERSEGURIDAD Kenneth Daniels- Widefense
10:55 – 11:40	Coffee Break – NETWORKING
11:40 – 12.10	LA AGONÍA DE LOS "TÉRMINOS Y CONDICIONES" Jessica Matus- Fundación Datos Protegidos
12:10 – 13:10	**MESA REDONDA: PROTECCIÓN DE DATOS** Modera: **Danielle Zaror** Integrantes de la mesa: **Felipe Harboe** – Senador de la República **Jeannette von Wolfersdorff** - Directora Ejecutiva del Observatorio del Gasto Fiscal en Chile **Alex Pessó -** Director Legal y de Asuntos Corporativos de Microsoft Chile **Juan Pablo González**- Abogado Ministerio del Interior
13:10-14:10	ALMUERZO
14:10 -14:40	DE LA CONFIANZA AL MÍNIMO PRIVILEGIO Guillermo Carrasco- Cyxtera
14:40 – 15:10	IDENTIFICANDO CÓMO LAS ORGANIZACIONES GESTIONAN LA INVERSIÓN EN CIBERSEGURIDAD José Lagos- Cybertrust
15:10-15:40	LA AMENAZA CONSTANTE DE LOS TROYANOS BANCARIOS André Goujón- Lockbits
15:40 -16:10	PHISHING EDUCATIVO: CONCIENTIZANDO A TRAVÉS DE HERRAMIENTAS DE HACKING Pablo Ramírez Ovalle y Ricardo Monreal Llop - Telefónica
16:10 -16:55	Coffee Break - NETWORKING
16:55 -17:25	OFFENSIVE THREAT INTELLIGENCE: ANTICIPANDO SITUACIONES DE RIESGO Germán Fernández- Cronup
17:25- 17:55	INTELIGENCIA ARTIFICIAL ASISTIENDO EN LA CIBERDEFENSA PROACTIVA Cristian Gorena- Deloitte
17:55 -18:25	LLEVANDO EL CUMPLIMIENTO A LA NUBE César Miranda- Ingenia Global
18:25- 18:55	SEGURIDAD EN SISTEMAS UBICUOS: IOT & TRUSTEDPALS Christian Fernández-Campusano - Universidad de Santiago de Chile

TALLERES Y CHARLAS TÉCNICAS

DÍA 1 -24 DE OCTUBRE

SALÓN ANTÁRTICA	SALÓN EUROPA	SALÓN CALBUCO
TALLER 1 11:15 – 13:15 "BLOCKCHAIN: ASPECTOS TEÓRICOS Y PRÁCTICOS" Eric Donders. ISC2 *TALLER GRATUITO/ CUPOS LIMITADOS	TALLER 3 11:15 – 13:15 "DE LA TEORÍA A LA PRÁCTICA EN EL PENTESTING" Sebastián Doll y Germán Fernández, Cronup	TALLER 4 11.30-13.30 "BENEFICIOS DEL CIFRADO GENERALIZADO DEL SISTEMA DE ARCHIVOS EN LINUXONE" Rodrigo Soave. S&A e IBM
TALLER 2 14:15 – 18:15 "CIBERSEGURIDAD PARA ABOGADOS" Jessica Matus, Fundación Datos Protegidos y Carlos Ormeño, 0rnitorrinco Labs.	TALLER 3-A 14:00 – 16:00 "RIESGOS, RETOS Y NECESIDAD DE PROTEGER DATOS SENSITIVOS EN EL MUNDO DIGITAL MODERNO" Daniel López Fernández, Thales TALLER 3-B 16:30 – 18:30 "COMO THREAT HUNTING AVANZADO MARCA LA DIFERENCIA EN LA PROTECCIÓN DE ENDPOINTS" Leone Tolesano, Carbon Black	CHARLAS TÉCNICAS 14:15-14:40 **AVANTIC** 14:45-15:10 **3IT** Cómo desarrollar software seguro "caso de éxito de la fábrica 3IT". Leonardo Toloza e Italo Massone. 15:15-15:40 **CRONUP** 15:45-16:10 **ASSERTIVA** 16:15-16:40 **CYBERTRUST** 16:45-17:10 **THALES** 17:15-17:40 **BUSINESS CONTINUITY** 17:45-18:10 **S&A** Servicios de Inteligencia de Seguridad. Víctor Barrera. 18:15-18:40 **HACKNOID**

TALLERES, CURSO Y CHARLAS TÉCNICAS

DÍA 2 -25 DE OCTUBRE

SALÓN ANTARTICA	SALÓN EUROPA	SALÓN CALBUCO
1ER CURSO DE DESARROLLO SEGURO DE SOFTWARE SAFECON 2019	TALLER 5 09:00 – 13:00 "CIBERSEGURIDAD FORENSE" Ariel Martin Torres y Ariel Luis Cessario, AAM+. Argentina **Requerimientos:** ***Los asistentes deben llevar su propio Computador** ***Conocimientos de seguridad y redes tcp/ip**	TALLER 8 11.30-13.30 EXTRACCION Y ANÁLISIS DE MEMORIA RAM Gustavo Ríos, Cybertrust *TALLER GRATUITO/ CUPOS LIMITADOS **Requerimientos:** **Los asistentes deben llevar su propio computador con la capacidad de correr el sistema operativo KALI LINUX (descargar previamente).**
	TALLER 6 14:15 – 16:15 "BASELINE DE CIBER-RESILIENCIA PARA LA INDUSTRIA 4.0" Jorge Olivares, Business Continuity **Requerimientos:** **Computador y conexión a internet**	TALLER 9 14.15-16.15 UN ENFOQUE INTEGRAL A RESPUESTA E INCIDENTE DE MANERA PRÁCTICA Cristian Venegas, Cisco
	TALLER 7 16:30 – 18:30 "TALLER PRÁCTICO PARA IDENTIFICAR Y PROTEGER INFORMACIÓN CRÍTICA BASADA EN CLASIFICACIÓN'' Sebastian Bonta y Alfonso Villalba, Kriptos *TALLER GRATUITO/ CUPOS LIMITADOS **Requerimientos:** **¨*No existen requerimientos especiales**	

ABSTRACTS CHARLAS:

DIA 1

24 de Octubre

ECOSISTEMAS DE CIBERSEGURIDAD DEL PACÍFICO SUR. Senador Kenneth Pugh

Análisis de los ecosistemas de ciberseguridad que se están generando en el pacífico sur. Comparación de la experiencia de Australia para ser adaptada y aplicada en Chile y formulación de una propuesta concreta para una institucionalidad, que permita avanzar en una política de "comercio digital seguro", de las economías del Pacifico APEC.

GDPR GAME CHANGERS AND SOLUTION FOR COMPLIANCE. Keynote Speaker Danielle Catteddu. CSA.

The European General Data Protection Regulation has been in force for over 1 year, its entering into force has generated a lot of debates, a great deal of investments from company seeking for compliance and pushed some government outside the EU to restart the national debate on the update of their local legislation.
But why GDPR has become so important? What are the game changers that has introduced and what's the real impact on organisations around the world?
In this presentation Mr Catteddu, the Global CTO of the Cloud Security Alliance, will discuss about the key principles of the GDPR, the challenges that several companies are facing to achieve compliance and finally some of the solutions that CSA has developed to support organisation that need or want to adhere to the GDPR.

CONVERGING IT-OT NETWORKS- THE POWER OF 100%VISIBILITY. Alejandro Dutto- Forescout Technologies

¿Puedes identificar lo que hay en tu red IT-OT? ¿Te preocupa que la seguridad necesitada impacte el tiempo de actividad de la producción de tu equipamiento? Aprenda de métricas reales de negocios y experiencias reales de clientes que comparten como el despliegue de una solución IT-OT para control y visibilidad entrega las bases fundamentales necesarias para protección y mitigación de riesgos.

PROTECCIÓN Y ANONIMIZACIÓN DE DATOS EN ECOSISTEMAS HÍBRIDOS. Sergio Muniz. Thales
Abstract Pendiente

BENEFICIOS DE UNA GESTIÓN INTEGRADA DE RIESGOS. Miguel Aranguren- Assertiva
Actualmente las empresas están bajo fuertes presiones para gestionar de forma eficaz los riesgos corporativos de forma que soporten el cumplimiento de los objetivos de negocio, mejoren el desempeño operativo, mitiguen los riesgos y mejoren su resiliência. Al mismo tempo, que aseguran el cumplimiento de las normas, regulaciones y estándares del mercado.
Conozca los beneficios de implementar una Gestión Integrada de Riesgos, que permita identificar, evaluar, tratar y monitorear los distintos tipos de riesgos con una visión integrada, logrando mejorar a capacidad de las empresas para lograr sus objetivos de negocio.

MODELO DE CONFIANZA CERO, LA NUEVA FORMA DE COMBATIR LAS AMENAZAS AVANZADAS. Ximena Tapia- Microsoft
De qué forma aplicar el modelo de arquitectura de seguridad basado en confianza cero, para proteger en forma transversal sus entornos nube

CIBERSEGURIDAD: LA PIEDRA ANGULAR DE LA TRANSFORMACIÓN DIGITAL. Orador por definir- Cisco
Abstract Pendiente

EL AWARENESS Y LA CULTURA ORGANIZACIONAL 3.0. Felipe Molina- 3IT

Esta charla busca dar respuesta a ese tipo de interrogantes, haciendo un recorrido por la evolución de la concientización y sensibilización de los riesgos de seguridad asociados a múltiples aspectos que afectan nuestras vidas. A través de un equipo multidisciplinario, se plantean distintas soluciones, entendiendo que todas las mejoras obedecen a un cambio de cultura en donde se trabaja desde la emoción y se busca transmitir un mensaje que pueda ser absorbido por la gente.

En este sentido, podremos ver cómo a través de la emoción se puede mejorar la entrega de la información para generar una cultura orientada a la ciberseguridad de forma cercana y amena. Y, finalmente, esperamos dar a conocer así, los 4 pilares que consideramos fundamentales: Educar, Comunicar, Practicar, Ser constantes (Practicidad).

ESTABLECIENDO PROGRAMAS DevSecOps QUE GENERAN RETORNOS TANGIBLES PARA EL NEGOCIO.
Edward Cook- Business Continuity

Las aplicaciones y la tecnología ya impulsan el crecimiento del negocio y continuarán desempeñando un papel cada vez más importante para diferenciar a las empresas de su competencia e impactar en el resultado final.
Las empresas con programas de seguridad de aplicaciones (AppSec) exitosos tienen una ventaja tremenda, ya que pueden hacer que las nuevas aplicaciones se pongan en producción de manera más rápida y económica que aquellos competidores que consideran a AppSec como mal necesario dentro del ciclo de desarrollo de software. Además, se benefician de menores costos operativos, menos fallas de seguridad y un riesgo muy reducido de brechas de seguridad que pueden costar millones en valor de marca y daños a la reputación.

LA IMPORTANCIA DE LA VISIBILIDAD EN LAS ESTRATEGIAS DE CIBERSEGURIDAD. Juan Vergara- Gigamon

El personal de tecnología manejan cada vez más, más herramientas de seguridad y para eso necesitan acceso a diferentes puntos del tráfico y copias del mismo. Necesitan que estas herramientas tengan toda la información importante para que esta pueda ser analizada y confiable. Por lo mismo se necesita información confiable y en tiempo real para que la copia sea autentica y exacta para que se pueda alimentar las herramientas necesarias. Tener una mayor visibilidad de red y la solución adecuada te permite optimizar no solo las herramientas de seguridad si no que también como usas el tiempo de tu personal de trabajo.

APLICACIÓN DE TEORÍA DE CONTROL E INTRODUCCIÓN DEL CONCEPTO DE RETROALIMENTACIÓN PARA UN NUEVO PARADIGMA EN CIBERSEGURIDAD. Ricardo Villadiego- Lumu Technologies

Una limitación significativa de la industria de ciberseguridad es su naturaleza reactiva, lo cual lleva a un ciclo vicioso "cyber cycle" de atacantes escaneando redes, desarrollando exploits y atacando sistemas y empresas detectando ataques, analizando exploits y 'parchando sistemas' Este presentación académica introduce el concepto de teoría de control para regular sistemas como un enfoque fundamental para desarrollar principios de ciberseguridad desde una perspectiva de la ciberdefensa.

ABSTRACTS CHARLAS:

DIA 2

INSIDE ATTACKS AND ZERO KNOWLEDGE NETWORKS. Jochen Kressin- Search Guard (Ponencia en Inglés)

¡No se puede confiar en nada dentro o fuera del perímetro de la red sin verificación! Las empresas están luchando para evitar violaciones de datos usando enfoques convencionales, invierten mucho tiempo y energía para proteger a sus redes contra ataques externos. Las VPN y los firewalls son la norma, pero la seguridad perimetral ya no es suficiente. El modelo Zero Trust Security mueve los mecanismos de control de acceso del perímetro de la red a los usuarios, dispositivos y sistemas reales.

LA PERSONA COMO EL ESLABÓN MÁS FUERTE DE LA CIBERSEGURIDAD. Kenneth Daniels- Widefense

El punto de interacción entre las personas y los datos puede socavar los sistemas de ciberseguridad de diseño más integral en un solo acto no intencional o malicioso. Nuestra última vulnerabilidad no es una forma de malware; Es nuestra naturaleza humana impredecible.
La observación del comportamiento cibernético permite a los profesionales de la seguridad determinar una línea de base para la normalidad, lo que luego hace posible identificar las acciones de riesgo que conducen a la pérdida de datos. Entender la intención puede diferenciar un intruso accidental de alguien maliciosamente planeando un incidente de seguridad.
Este enfoque requiere sistemas inteligentes y colaboración transparente entre las partes interesadas de una organización. Proteger el punto humano- donde las personas interactúan con datos empresariales críticos y propiedad intelectual- es una oportunidad para proteger verdaderamente a los empleados y los datos empresariales críticos.

LA AGONÍA DE LOS "TÉRMINOS Y CONDICIONES". Jessica Matus- Fundación Datos Protegidos
Abstract pendiente

DE LA CONFIANZA AL MÍNIMO PRIVILEGIO. Guillermo Carrasco- Cyxtera

Hoy en día más organizaciones de cualquier tamaño son víctimas del ciber crimen, las soluciones tradicionales han quedado expuestas ante ataques sofisticados y mejor elaborados, los perímetros se quedan cortos en ambientes híbridos como la nube, premisas, centro de datos, usuarios remotos, etc..
Ante esta situación es necesario cambiar el enfoque hacia el aseguramiento de las comunicaciones sin importar su origen, implementando una estrategia de microsegmentación que permita tener accesos seguros, puntuales y basados en el contexto de usuario y no solo en la red, aplicando esquemas multifactoriales que permitan tener control sobre el QUIEN, CON QUE, A DONDE Y CUANDO.
Ya no podemos pensar solo en tecnología y procesos, debemos ir más allá de la remediación, debemos comenzar a pensar en cuanto tiempo y paciencia tiene un atacante para lograr su objetivo, partiendo de esto, la postura de ciberseguridad debe cambiar por algo más práctico, de fácil despliegue y centrado en 3 principios: Identidad, privilegios dinámicos y microsegmentación.

IDENTIFICANDO CÓMO LAS ORGANIZACIONES GESTIONAN LA INVERSIÓN EN CIBERSEGURIDAD José Lagos- Cybertrust

Esta charla se orienta a entender como tradicionalmente las organizaciones definen sus inversiones en Ciberseguridad, pasando desde los métodos tradicionales a métodos más avanzados, identificando las últimas técnicas disponibles en esta materia.

LA AMENAZA CONSTANTE DE LOS TROYANOS BANCARIOS. André Goujón- Lockbits

Estado de la banca en América Latina
Amenazas informáticas que afectan al sector financiero
Grupo Lazarus y modus operandi
Emotet, Zbot, SpyBanker y otros malware que afectan la banca
Demo Zeus

PHISHING EDUCATIVO: CONCIENTIZANDO A TRAVÉS DE HERRAMIENTAS DE HACKING Pablo Ramírez Ovalle y Ricardo Monreal Llop – Telefónica

Desarrollar el concepto de phishing y por qué sigue siendo uno de los vectores de ataques más comunes hoy en día. Además de mostrar cómo, con un poco de desarrollo interno y usando las mismas técnicas, podemos generar una campaña de concientización.
Según reporte de Verizon (https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf):
- el 4% de las personas van a hacer click en una campaña de phishing
- pasan 16 minutos para que la primera persona caiga
- pasan 28 minutos para que alguien reporte un phishing, según reporte de Proofpoint (https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q119-quarterly-threat-report-0528.pdf)
- URL maliciosas en correos superan 5 a 1 a los adjuntos maliciosos
Con el desarrollo de este tipo de ataques necesitamos definir procesos y roles que se encarguen de defender y reaccionar contra estos problemas. Una de las mejores defensas es entregar conocimiento a las personas de la organización a través de una prueba controlada, un phishing educativo.
En el laboratorio de investigación desarrollamos una prueba de concepto para phishing educativo dependiendo de los objetivos del ataque (robo de credenciales o infección directa), encontrando datos muy interesantes.

OFFENSIVE THREAT INTELLIGENCE: ANTICIPANDO SITUACIONES DE RIESGO. Germán Fernández- Cronup

Presentaremos, el cómo el conocimiento del mundo técnico (hackers) contribuye en la estrategia de Ciberseguridad corporativa, y cómo un proceso de Threat Intelligence aporta valor en la detección, visibilidad y capacidad de respuesta temprana a las amenazas de hoy en día.

En esta presentación se mostrarán casos reales de Threat Hunting, que han permitido reconocer tácticas, técnicas y procedimientos (TTP's) de adversarios que atacan la región, que han permito anular sus campañas de ataque.

Anticipar situaciones de riesgo es la clave para apoyar los procesos de toma de decisions y que entregue la oportunidades de protegerse contra las amenazas.

INTELIGENCIA ARTIFICIAL ASISTIENDO EN LA CIBERDEFENSA PROACTIVA. Cristian Gorena- Deloitte

Los ciber-adversarios evolucionan constantemente las tácticas y técnicas que utilizan para comprometer a sus objetivos. La pregunta ya no se basa en si seremos un objetivo, sino en qué intentará hacer un atacante una vez que intente infiltrar nuestras redes.

LLEVANDO EL CUMPLIMIENTO A LA NUBE César Miranda- Ingenia Global

1.- Informe meteorológico: nublado con probabilidad de riesgo

2.- Principales amenazas de seguridad y privacidad en la nube

2.1 Según ENISA

2.2 Según CSA

2.3 Según NCSC UK

3.- Normas ISO para la seguridad y privacidad en la nube

3.1 ISO 27017 - Gestión de riesgos en la nube

3.2 ISO 27018 - Protección de información de identificación personal en nubes públicas

3.3 Evaluaciones de riesgos para aplicaciones en la nube

3.4 Mejores prácticas seguridad en la nube y riesgo de privacidad

4. Herramientas y técnicas

4.1 Responsabilidades compartidas de seguridad en la nube

4.2 Evaluación de una política de seguridad y privacidad en la nube

4.2.1 ISO 27017 / 27018 Controles Referenciados (ISO 27001 Anexo A)

4.2.2 Lista de verificación de evaluación de Azure

4.2.3 Resumen de hallazgos y mitigaciones de riesgos

4.2.4 CASB

4.2.5 CWPP

4.2.6 CSPM

SEGURIDAD EN SISTEMAS UBICUOS: IOT & TRUSTEDPALS
Christian Fernández-Campusano - Universidad de Santiago de Chile
Abstract pendiente.

ABTRACTS TALLERES

“BLOCKCHAIN: ASPECTOS TEÓRICOS Y PRÁCTICOS” Eric Donders. ISC2

En la actualidad el uso de Blockchain está cada vez más siendo utilizado en otras áreas diferentes a las ya conocidas criptomonedas (bitcoin) tales como; Identidad, Auditoría, Forense, Registro Notariales, etc. Es por esto que es importante entender sus fundamentos y así sus potenciales aplicaciones.
El taller anatomía de Blockchain permite revisar los puntos fundamentales y teóricos de tecnología Blockchain y través de demostraciones desarrolladas en el taller validar como estos aspectos se aplican en el ámbito de la tecnologías de Información
Se revisarán también las potencialidades de la tecnologías revisando casos de usos
El taller se desarrolla principalmente en cuatros módulos
Modulo I: Entendimiento Básico de Blockchain
Modulo II: Los Fundamentos Teóricos de Blockchain
Modulo III: Revisión de Casos de Usos de Blockchain
Modulo IV: Revisión de la Operación de la Tecnología a través de una demostración guiada durante el Taller

“CIBERSEGURIDAD PARA ABOGADOS” Jessica Matus, Fundación Datos Protegidos y Carlos Ormeño, 0rnitorrinco Labs.

1. La importancia de la ciberseguridad:

a. Conceptos básicos: hardware, software, internet.
b. ¿Cómo nos afecta la ciberseguridad a los abogados?

2. Riesgos en el mundo del internet: Ingeniería social, , vulnerabilidades, malware y acoso.

a. Ingeniería social: phishing, catfish, vishing.
b. Malware: spyware, hijacking, keyloggers y stealers, botnets, ransomware.
c. Acoso en internet: doxxing, robo de identidad.
d. Figuras penales relacionadas al uso de internet y sistemas informáticos.
e. La problemática actual de las figuras atípicas, relación con el derecho comparado.

3. ¿Qué información existe sobre mi en internet? Ciberseguridad básica:

a. La importancia de tener un buen firewall y una buena suite de seguridad instalada.
b. Portátil, cómodo, siempre bajo tu poder: Privilegiar el hardware que podemos llevar fácilmente de un lado a otro.
c. ¿Puedo pagar con efectivo?: Los riesgos que pueden significar las tarjetas de crédito y/o débito.
d. Si no es necesario, no lo instales: Hábitos saludables sobre instalación de software.
e. Hábitos de seguridad en redes sociales.

4. Seguridad digital básica: Herramientas.

a. Contraseñas: Cómo crear y memorizar contraseñas seguras, una distinta para cada plataforma, cómo usar un gestor de contraseñas, y hábitos saludables para el manejo de tus contraseñas.
b. Correos electrónicos: Correos desechables, enviar correos desde redes públicas, cifrado de correo, Thunderbird y PGP.
c. Navegar en internet: SSL/TSL, TOR, y VPN; medidas de emergencia si nos tenemos que conectar a redes públicas.
d. Herramientas para smartphones: TOR, OSTN+CsipSimple, Keybase. ¿Qué información guarda mi celular?
e. Disco duro: TrueCrypt y Limpieza Total de Datos.
f. Un Sistema Operativo Viviente: TAILS.

“DE LA TEORÍA A LA PRÁCTICA EN EL PENTESTING” Sebastián Doll y Germán Fernández, Cronup

- Que es el Pentesting
- Tipos de auditoria
- Fases de un Test de Intrusión
- Metodologías
- Práctica sobre maquina vulnerable
- Explotación Apache
- Explotación Tomcat
- Explotación Elasticsearch
- Explotación Jenkins
- Desafío final Práctico de lo aprendido

"RIESGOS, RETOS Y NECESIDAD DE PROTEGER DATOS SENSITIVOS EN EL MUNDO DIGITAL MODERNO" Daniel López Fernández, Thales

En la actualidad con la marcada tendencia por compartir datos personales en diferentes medios digitales así como consumir servicios en la nube, la experiencia de usuario su principal y la disponibilidad de los servicios es el objetivo principal de las empresas detrás de dichos servicios.

Sin embargo se ha omitido un elemento importante que es la protección de los datos sensitivos de los clientes que son recibidos, transmitidos, procesados y almacenados con el uso de dichos servicios, en consecuencia se han publicado diferentes brechas de seguridad donde dichos datos sensitivos fueron expuestos por personas que buscan un fin lucrativo, reconocimiento personal o dañar la reputación de una empresa.

La solución a esta problemática es la protección de datos mediante diferentes técnicas que van más a allá de la seguridad perimetral, estas herramientas son el cifrado y tokenización de la información sensitiva así como agregar mecanismos de autenticación fuerte a los recursos privilegiados.

"COMO THREAT HUNTING AVANZADO MARCA LA DIFERENCIA EN LA PROTECCIÓN DE ENDPOINTS" Leone Tolesano, Carbon Black
Desde reputación de archivos hasta heurística, análisis de código estático, hash difuso (fuzzy hash), inteligencia artificial y análisis de comportamiento de eventos en tiempo real, hablaremos de la evolución de la protección de endpoints con ejemplos prácticos y escenarios del mundo real.

"BENEFICIOS DEL CIFRADO GENERALIZADO DEL SISTEMA DE ARCHIVOS EN LINUXONE" Rodrigo Soave. S&A e IBM

En este taller veremos cuán simple es crear volúmenes en Linux y usar la tecnología de procesador LinuxONE para encriptar todo el volumen usando las claves de la tarjeta HSM.
Veremos cuán sofisticados son los ataques y el objetivo final de los piratas informáticos siempre será robar datos importantes.Y con el cifrado generalizado de LinuxONE, veremos que ahora tenemos una gran arma para combatir el robo de datos abiertos que afecta a todos los ejecutivos de TI y Seguridad del mundo.
También descubriremos que el procesamiento para cifrar y descifrar datos en el volumen cifrado no sufre ninguna penalización por el rendimiento de LinuxONE.

"CIBERSEGURIDAD FORENSE" Ariel Martin Torres y Ariel Luis Cessario, AAM+. Argentina

El incremento exponencial de los ciberdelitos y el modus operandi con que se desarrollan, hacen que los dispositivos y tecnología empleada, se conviertan en testigos mudos de lo que ha ocurrido y su vinculación como medios de prueba en el marco de investigaciones judiciales.
Este tipo de dispositivos deben ser analizados en consonancia con las reglas de buena práctica forense reconocidas internacionalmente, a fin de identificar, preservar, analizar y presentar evidencias válidas en el proceso legal, lo que representa en muchas ocasiones un desafío para el investigador en informática forense.
Por este motivo, el presente curso tiene como finalidad dotar a los investigadores de aquellos conocimientos básicos y necesarios en la materia, para construir bases sólidas de conocimiento, sobre el que deberá apuntalar futuras capacitaciones en el empleo de las herramientas forenses a fin de evacuar las necesidades emergentes de la actividad operativa y el quehacer pericial propiamente dicho.

“BASELINE DE CIBER-RESILIENCIA PARA LA INDUSTRIA 4.0” Jorge Olivares, Business Continuity

Existe carencia de aplicaciones prácticas que apoyen metodológicamente la conformación inicial de un Sistema de gestión de Ciberseguridad y Continuidad Operacional para los Sistemas de Automatización y Control Industrial, integrado con los sistemas de gestión corporativos.

El presente Taller busca entregar herramientas concretas que permitan identificar y avanzar en las etapas iniciales de conformación de un marco integral de gestión de mejora continua para el gobierno y el marco normativo y de controles de ciberseguridad y continuidad de las tecnologías de operación de las redes industriales.

Asimismo, se hará hincapié en mecanismos que permitan acercar las visiones y trabajo cooperativo de los equipos de ciberseguridad de los ámbitos Administrativo, Comercial e Industrial.

Entre los contenidos teóricos/prácticos destacan:

- Revisión de los principios de ciberseguridad, continuidad operacional y ciber-resiliencia en su aplicación a redes industriales.
- “Tanatología” a los paradigmas obsoletos de una red industrial aislada.
- Revisión y aplicación de recomendaciones de informes de ciber-resiliencia del Foro Económico Mundial y la OEA.
- Revisión y aplicación de un modelo de madurez del relacionamiento entre gestión y gobierno de ciberseguridad TI (redes administrativas) y ciberseguridad TO (redes de control).
- Esbozo de estructuración del gobierno integrado de ciberseguridad y continuidad operacional para entornos administrativo, comercial e industrial.
- Esbozo de definición de una política de ciberseguridad y ciber-resiliencia industrial.

“TALLER PRÁCTICO PARA IDENTIFICAR Y PROTEGER INFORMACIÓN CRÍTICA BASADA EN CLASIFICACIÓN’’
Sebastian Bonta y Alfonso Villalba, Kriptos

Taller práctico donde se profundizará en métodos y herramientas que faciliten las tomas de decisión al momento de priorizar el presupuesto y las actividades relacionadas con la gestión de la estrategia de Ciberseguridad basados en Frameworks y Normativas tipo NIST, ISO 27001, PCI, otros.
A través del taller 100% práctico, los participantes obtendrán indicadores sobre la gestión de información de sus empresas en base a algoritmos implementados en + de 45 empresas de LATAM.
Simularemos la distribución de su información según su nivel de confidencialidad, el valor económico de la información y su probabilidad de fuga.
Concluimos con una presentación final donde cada uno de los participantes podrán exponer los resultados obtenidos con nuestro simulador aplicado a su propia empresa y el impacto que tiene para su presupuesto y estrategia de ciberseguridad.
Importante: mantendremos y respetaremos el no uso de material publicitario generando material en marca blanca.

“EXTRACCION Y ANÁLISIS DE MEMORIA RAM” Gustavo Ríos, Cybertrust
Pending

“UN ENFOQUE INTEGRAL A RESPUESTA E INCIDENTE DE MANERA PRÁCTICA” Cristian Venegas, Cisco
Pending